

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

NICHOLAS CIMAGLIO, on behalf of himself  
and all others similarly situated,

Plaintiff,

v.

WARNER MUSIC GROUP CORPORATION,

Defendant.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Nicholas Cimaglio (“Plaintiff”) brings this action on behalf of himself and all others similarly situated against Defendant Warner Music Group Corporation (“WMG” or “Defendant”). Plaintiff makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to the allegations specifically pertaining to himself, which are based on personal knowledge.

**NATURE OF THE ACTION**

1. WMG is one of the “big three” recording companies and the third largest in the global music industry.

2. Between April 25, 2020 and August 5, 2020, WMG was the subject of a data breach due to its negligent failure to properly safeguard the information of its customers. The data breach exposed the names, email addresses, telephone numbers, billing addresses, shipping addresses, and payment card details (card number, CVC/CVV and expiration date) (collectively, the “personal identifying information” or “PII”) of WMG customers.<sup>1</sup>

---

<sup>1</sup> NOTICE OF DATA BREACH, [https://oag.ca.gov/system/files/California\\_Consumer%20Letter.pdf](https://oag.ca.gov/system/files/California_Consumer%20Letter.pdf).

3. Plaintiff brings this class action on behalf of himself and all others similarly situated for actual and statutory damages, as well as punitive damages and equitable relief, to fully redress the widespread harm WMGs' wrongful acts and omissions have unleashed.

### **THE PARTIES**

4. Plaintiff Nicholas Cimaglio is a citizen of California who resides in Solano County, California. On June 30, 2020, Mr. Cimaglio purchased merchandise on [www.greenday.com](http://www.greenday.com), which is owned and operated by Defendant. As part of this transaction, Mr. Cimaglio entrusted his PII, including his name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date) to Defendant. When entrusting his PII to Defendant, Mr. Cimaglio reasonably believed that his PII would be securely stored and protected against unauthorized access. In fact, Defendant represented in its Privacy Policy that it uses "reasonable physical, technical and administrative measures to protect Personal Information under our control."

5. In September 2020, Mr. Cimaglio received a letter from Defendant informing him that his PII—including his name, email address, telephone number, billing address, shipping address, and payment card details—was accessed and extracted in a data breach. Mr. Cimaglio now faces a substantial and imminent risk of fraud, identity theft, and long-term adverse effects as a result of his PII being compromised. In fact, Mr. Cimaglio was already the victim of identity theft in August 2020, shortly after his purchase, when Mr. Cimaglio incurred fraudulent charges on his credit card. This was the same credit card that Mr. Cimaglio used to purchase memorabilia from the WMG store. As part of dealing with the fraudulent charge, Mr. Cimaglio was forced to spend time cancelling his credit card and receiving a new one. Upon information and belief, these fraudulent charges were the result of the WMG data breach.

6. Defendant Warner Music Group Corporation is a Delaware corporation with a principal place of business at 1633 Broadway, New York, New York 10019.

### **JURISDICTION AND VENUE**

7. This Court has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 members of the Class, the aggregate amount in controversy exceeds \$5,000,000.00, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in New York.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391 Defendant's principal place of business is in this District.

### **FACTUAL ALLEGATIONS**

#### **I. BACKGROUND ON DATA BREACHES**

10. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.<sup>2</sup>

11. A data breach can occur in numerous ways. One way that a data breach can occur, and most relevant to this action, is through skimming. Skimming occurs when "thieves steal payment data directly from the consumer's payment card or from the payment infrastructure at a merchant location."<sup>3</sup> Skimming can also occur when an unauthorized user

---

<sup>2</sup> Julian De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 24, 2019), <https://digitalguardian.com/blog/history-data-breaches>.

<sup>3</sup> PCI SECURITY STANDARDS COUNCIL, SKIMMING PREVENTION OVERVIEW OF BEST PRACTICES FOR MERCHANTS (2009), [https://www.pcisecuritystandards.org/documents/skimming\\_prevention\\_overview\\_one\\_sheet.pdf](https://www.pcisecuritystandards.org/documents/skimming_prevention_overview_one_sheet.pdf).

inserts a virtual credit card skimmer or scraper (known as “formjacking”) into a web application (such as the shopping card) in order to scrape or steal credit card information. This information can then be used to make fraudulent purchases, or sold for profit to other criminals.<sup>4</sup> This method of skimming is the *modus operati* of a criminal hacker group called “Magecart.”<sup>5</sup>

12. The purpose of skimming “is to commit fraud.” “[T]he threat is serious, and it can hit any merchant’s environment.”<sup>6</sup> The PII of Plaintiff and class members are certain to be used for nefarious purposes.

13. Data breaches are becoming increasingly more common and harmful. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed.<sup>7</sup> In 2019, 3,800 data breaches were reported, with at least 4.1 billion total records exposed.<sup>8</sup> The average cost of a data breach in the United States in 2019 was \$8.19 million.<sup>9</sup>

14. Consumers are harmed in a variety of ways by data breaches. First, consumers are harmed financially. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report, the average cost of a data breach per consumer was \$150 per record.<sup>10</sup> However, other estimates have placed the costs even higher. The 2013 Norton Report estimated that the

---

<sup>4</sup> Tara Seals, *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, THREATPOST, Aug. 28, 2019, <https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/>.

<sup>5</sup> *Id.*

<sup>6</sup> PCI SECURITY STANDARDS COUNCIL, SKIMMING PREVENTION OVERVIEW OF BEST PRACTICES FOR MERCHANTS.

<sup>7</sup> Julian De Groot, *The History of Data Breaches*.

<sup>8</sup> Dan Rafter, *2019 Data Breaches: 4 Billion Records Breached So Far*, NORTON BY SYMANTEC, <https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>.

<sup>9</sup> Chris Brook, *What’s the Cost of a Data Breach in 2019*, DIGITAL GUARDIAN (July 30, 2019), <https://digitalguardian.com/blog/whats-cost-data-breach-2019>.

<sup>10</sup> *Id.*

average cost per victim of identity theft—a common result of data breaches—was \$298 dollars.<sup>11</sup>

And in 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade Commission (“FTC”) and indicated that the median out-of-pocket cost to consumers for identity theft was \$375.<sup>12</sup>

15. Identity theft is one of the most problematic harms resulting from a data breach. With access to an individual’s PII, criminals can do more than just empty a victim’s bank account – they can also commit all manner of fraud, including obtaining a driver’s license or official identification card in the victim’s name but with the thief’s picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim’s name. Identity thieves may even give the victim’s personal information to police during an arrest, resulting in an arrest warrant being issued in the victim’s name.<sup>13</sup>

16. Consumers are also harmed by the time they spend rectifying the effects of a data breach. A Presidential identity theft report from 2007 states that:

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts, open new ones, and dispute charges with individual creditors.<sup>14</sup>

---

<sup>11</sup> NORTON BY SYMANTEC, 2013 NORTON REPORT 8 (2013), [https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf).

<sup>12</sup> *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin report).

<sup>13</sup> See *Warning Signs of Identity Theft*, Federal Trade Commission, <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>.

<sup>14</sup> U.S. FEDERAL TRADE COMMISSION, THE PRESIDENT’S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 11 (2007), <https://www.ftc.gov/sites/default/>

17. Further, the effects of a data breach on consumers are not temporary. In a report issued by the U.S. Government Accountability Office (“GAO”), the GAO found that “stolen data may be held for up to a year or more before being used to commit identity theft,” and “fraudulent use of [stolen information] may continue for years” after the stolen information is posted on the Internet.<sup>15</sup> In fact, consumers suffer 33% of the harm from a data breach after the first year.<sup>16</sup> Thus, consumers can lose years’ worth of time dealing with a data breach.

## II. THE WMG DATA BREACH

18. Between April 25, 2020 and August 5, 2020, WMG was the subject of a data breach.

19. Upon information and belief, the data breach was conducted through a prolonged, Magecart-style skimming attack across numerous websites operated by WMG. In other words, hackers implanted virtual software on the checkout pages of WMG’s websites, which allowed the unauthorized third party to acquire a copy of the PII entered by customers in WMG’s websites.

20. WMG did not learn of this skimming attack until August 5, 2020. At this time, WMG ascertained that the data breach divulged the names, email addresses, telephone numbers, billing addresses, shipping addresses, and payment card details (card number, CVC/CVV and expiration date) of WMG customers.<sup>17</sup>

---

files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

<sup>15</sup> *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION (2007)).

<sup>16</sup> Larry Ponemon, *What’s New in the 2019 Cost of a Data Breach Report*, SECURITY INTELLIGENCE, <https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/>.

<sup>17</sup> NOTICE OF DATA BREACH.

21. WMG began mailing out letters to affected individuals in September 2020. Upon information and belief, as of the date of this Complaint, not all individuals have received their notice letter of the data breach.

22. The data breach affected individuals across the United States.

23. None of the individuals whose PII was accessed, authorized such access or extraction.

24. WMG represents in its Privacy Policy that it uses “reasonable physical, technical and administrative measures design to protect Personal Information under our control.”<sup>18</sup> Despite this representation, WMG failed to take reasonable measures to protect the personal information of Plaintiffs and members of the Class, included the following:

- (a) Failing to maintain appropriate technological and other systems to prevent unauthorized access. Despite WMG’s claim that it uses “reasonable ... technical ... measures” to protect sensitive data, WMG’s system was still subject to a data breach. Indeed, WMG failed to encrypt customer PII on its checkout page, which allowed the data breach to occur. Further, WMG was previously subject to a data breach in 2017,<sup>19</sup> yet still left its systems open to vulnerabilities. Defendant should have kept its systems up to date to avoid the data breach.
- (b) Failing to recognize the data breach in a timely manner. Despite WMG’s claim that it uses “reasonable physical ... and administrative measures” to protect sensitive data, WMG failed to detect the skimming attack until August 5, 2020, almost four months after it occurred. Had WMG been more diligent in surveying

---

<sup>18</sup> WMG PRIVACY POLICY, <https://www.wmg.com/privacy/wmg>.

<sup>19</sup> Sarah Coble, *Warner Music Group Discloses Data Breach*, INFOSECURITY, Sept. 4, 2020, <https://www.infosecurity-magazine.com/news/warner-music-group-discloses-data/>

its systems, the data breach would not have occurred, or WMG would have caught the data breach earlier and minimized the extent of the data breach.

25. Although WMG is offering individuals affected by the data breach complimentary identity protection services, these “remedies” are inadequate and too little too late. First, much of the harm from a data breach can happen years after the data breach occurs. In fact, identity thieves may simply calendar the date that the credit monitoring services are set to expire and act then, as “they don’t mind hanging on until they get over that time period.”<sup>20</sup> Second, this offer fails to reimburse consumers for their out-of-pocket expenses and lost time that they spent rectifying the effects of the data breach. Thus, the remedial action by WMG is inadequate to rectify the harm caused to Plaintiff and others similarly situated by the data breach.

26. Plaintiff brings this action on behalf of himself, the Class, and the Subclass for actual and statutory damages, as well as punitive damages for: (i) negligence, (ii) negligent misrepresentation, (iii) negligence per se for violation of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, (iv) breach of contract, (v) violations of New York General Business Law (“GBL”) § 349, and (vi) violations of New York GBL § 350.

### **CLASS ACTION ALLEGATIONS**

27. Plaintiff seeks to represent a class defined as all persons or business entities in the United States whose PII was entered on websites operated by WMG that were compromised as a result of the data breach (the “Class”). Excluded from the Class are Defendant, its affiliates, employees other than those affected by the data breach, officers and directors, and the Judge(s) assigned to this case.

---

<sup>20</sup> Alicia Grzadkowska, *Consumers’ Data Exposed for Years Following Breach Incidents*, INSURANCE BUSINESS, Sept. 19, 2019, <https://www.insurancebusinessmag.com/us/news/cyber/consumers-data-exposed-for-years-following-breach-incidents-178390.aspx>.

28. Plaintiff also seeks to represent a subclass consisting of Class members who reside in California (the “Subclass”).

29. Collectively, the Class and Subclass shall be referred to as the “Classes.”

30. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

31. At this time, Plaintiff does not know the exact number of members of the Classes. However, given the nature of the claims and the size of Defendant’s business, Plaintiff believes that the members of the Classes are so numerous that joinder of all members is impracticable.

32. Common questions of law and fact exist as to all members of the Classes. The data breach was generally applicable to all members of the Classes and arose from a common set of acts and omissions by Defendant without regard to the nature or identity of individual members of the Classes, thereby making appropriate relief with respect to the Classes as a whole.

33. The questions of law and fact common to the Class include:

- (a) Whether Defendant owed a duty to the members of the Classes under federal or state law to protect the PII, provide timely notice of the unauthorized access, provide timely and accurate information as to the extent of the compromised PII, and provide meaningful and fair redress;
- (b) Whether Defendant breached such a duty;
- (c) Whether Defendant’s breach provided the means for the data breach;
- (d) Whether Defendant was negligent in failing to design, employ, and maintain adequate security systems and protocols;
- (e) Whether Defendant’s negligence provided the means for the data breach;

- (f) Whether Defendant knew or reasonably should have known of the vulnerabilities in its systems that allowed for the unauthorized access;
- (g) Whether Defendant falsely represented that it uses “reasonable physical, technical and administrative measures designed to protect Personal Information under our control”;
- (h) The appropriate injunctive and related equitable relief for the Class; and
- (i) The appropriate class-wide measure of damages for the Class.

34. Plaintiff’s claims are typical of the claims of the members of the Class, and Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff and all members of the Class are similarly affected by Defendant’s wrongful conduct in that their PII has been exposed to criminal third parties without their authorization.

35. Plaintiff’s claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes.

36. Plaintiff’s interests are coincident with, and not antagonistic to, those of the other members of the Classes.

37. Plaintiff is represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation, including data breaches.

38. The questions of law and fact common to the members of the Classes predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

39. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently

and without the unnecessary duplication of evidence, effort, and expense of numerous individual actions. The benefits of proceeding as a class, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

40. The prosecution of separate actions by individual members of the Classes is not feasible and would create a risk of inconsistent or varying adjudications.

### **COUNT I** **Negligence**

41. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

42. Plaintiff brings this claim on behalf of himself and all members of the proposed Classes against Defendant.

43. Defendant had and continues to have a duty to Plaintiff and members of the Classes to safeguard and protect their PII. Defendant created this duty by requiring Plaintiff and members of the Classes to provide their PII, storing the PII, using the PII for commercial gain, and making representations in its Privacy Policy that it uses “reasonable physical, technical and administrative measures designed to protect Personal Information under our control.”

44. Defendant’s duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies, and intrusion detection and reporting systems sufficient to protect the PII from unauthorized access and to promptly alert Defendant to any such access and enable it to determine the extent of any compromised PII.

45. Had Defendant adequately designed, employed, and maintained appropriate technological and other systems, the PII would not have been compromised or, at a minimum, Defendant would have known of the unauthorized access sooner and would be able to accurately

inform Plaintiff and the other members of the Classes of the extent to which their PII has been compromised.

46. Defendant breached its duties of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to minimize the PII that any intrusion could compromise, and failing to detect the data breach in a timely manner to avoid or minimize the effects of the data breach.

47. Defendant's breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiff and the members of the Classes without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized users.

48. Defendant's breach of its duties has directly and proximately injured Plaintiff and members of the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

49. Plaintiff and the members of the Classes are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

## **COUNT II**

### **Negligent Misrepresentation**

50. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

51. Plaintiff brings this claim on behalf of himself and all members of the proposed Classes against Defendant.

52. Defendant represented in its Privacy Policy that it uses “reasonable physical, technical and administrative measures designed to protect Personal Information under our control.”

53. These representations were for the express purpose of protecting Plaintiff’s and members of the Classes’ PII, and created an affirmative duty to use “reasonable physical, technical and administrative measures designed to protect Personal Information.”

54. Defendant made these representations in the ordinary course of its regular business with the intent to induce Plaintiff and members of the Classes to supply their PII to Defendant for the purposes of conducting transactions with Defendant.

55. Defendant knew that Plaintiff and members of the Classes would rely on the above-referenced representations in supplying their PII to Defendant for the purposes of conducting transactions with Defendant.

56. Plaintiffs and members of the Classes justifiably relied on Defendant’s representations regarding the security of their PII in choosing to provide their PII to Defendant.

57. Defendant violated these representations by failing to use reasonable measures to secure the PII of Plaintiff and members of the Classes. Specifically, Defendant failed to maintain appropriate technological and other systems to prevent unauthorized access, failed to minimize the PII that any intrusion could compromise, and failed to detect the data breach in a timely manner to avoid or minimize the effects of the data breach.

58. It was reasonably foreseeable in that Defendant knew or should have known that its failure to implement reasonable measures to protect the PII of Plaintiff and members of the Classes would result in the data breach of such information.

59. The release and disclosure of Plaintiff's and members of the Classes' PII to third parties was without Plaintiff's and members of the Classes' authorization or consent.

60. Defendant's breach of its duties has directly and proximately injured Plaintiff and members of the Classes including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

**COUNT III**  
**Negligence *Per Se* For Violation of the Federal Trade Commission Act,**  
**15 U.S.C. § 45**

61. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

62. Plaintiff brings this claim on behalf of himself and all members of the proposed Classes against Defendant.

63. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce." The FTC has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5.

64. The FTC has provided guidance on how businesses should protect against data breaches, including: protect the personal customer information they acquire; properly dispose of personal information that is not necessary to maintain; encrypt information stored on computer networks; understand their network's vulnerabilities; and install vendor-approved updates to address those vulnerabilities. FTC guidance also recommends that businesses use an intrusion

detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.

65. Plaintiff and members of the Classes are within the class of persons Section 5 of the FTCA was intended to protect.

66. The harm that has occurred is the type of harm the FTCA was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and members of the Classes.

67. Defendant owed a duty to Plaintiffs and members of the Class under the Section 5 of the FTCA.

68. Defendant breached its duty under Section 5 of the FTCA by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to minimize the PII that any intrusion could compromise, and failing to detect the data breach in a timely manner to avoid or minimize the effects of the data breach.

69. Defendant's breach of its duties has directly and proximately injured Plaintiff and members of the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

70. Plaintiff and the members of the Classes are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

**COUNT IV**  
**Breach of Contract**

71. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

72. Plaintiff brings this claim on behalf of himself and all members of the proposed Classes against Defendant.

73. Defendant entered into contracts with Plaintiff and members of the Classes to conduct transactions.

74. These contracts included or otherwise incorporated Defendant's Privacy Policy, in which Defendant represented that it uses "reasonable physical, technical and administrative measures designed to protect Personal Information under our control."

75. Defendant has breached these contracts by failing to use "reasonable physical, technical and administrative measures designed to protect Personal Information under our control," including by failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to minimize the PII that any intrusion could compromise, and failing to detect the data breach in a timely manner to avoid or minimize the effects of the data breach.

76. Plaintiff and members of the Classes have suffered damages as a result of Defendant's breach, including through identity theft and expenses incurred combating identity theft.

**COUNT V**  
**Violation Of New York GBL § 349**

77. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

78. Plaintiff brings this claim individually and on behalf of the proposed Classes against Defendant.

79. New York's General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

80. In its provision of services throughout the State of New York, Defendant conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

81. Plaintiff and members of the Classes are consumers who conducted transactions with Defendant for their personal use.

82. The Terms of Use on Defendant's website "is governed by and shall be construed in accordance with the laws of the State of New York."<sup>21</sup> Further, Defendant was paid in New York, where it is headquartered, and customer communications are directed to Defendant's offices in New York. Accordingly, out-of-state plaintiffs have standing to sue Defendant under GBL § 349.

83. By the acts and conduct alleged herein, Defendant has engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, misrepresenting that Defendant used "reasonable physical, technical and administrative measures to protect Personal Information under our control" when in fact Defendant did not.

84. The foregoing deceptive acts and practices were directed at consumers.

85. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the ability and measures taken by Defendant to safeguard consumer PII, and to induce consumers to enter transactions with Defendant.

---

<sup>21</sup> WMG TERMS OF USE § 22, <https://www.wmg.com/terms-of-use>.

86. By reason of this conduct, Defendant engaged in deceptive conduct in violation of GBL § 349.

87. Defendant's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiff and members of the Classes have sustained from having provided their PII to Defendant, which was exposed in the data breach.

88. As a result of Defendant's violations, Plaintiff and members of the Classes have suffered damages because: (a) they would not have provided their PII to Defendant had they known Defendant did not use "reasonable physical, technical and administrative measures to protect Personal Information under our control"; (b) their PII has been devalued as a result of being exposed in the data breach; and (c) Plaintiff and members of the Classes must spend considerable time and expenses dealing with the effects of the data breach, and are now at greater risk for future harm stemming from the data breach.

89. On behalf of himself and other members of the Classes, Plaintiff seeks to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

**COUNT VI**  
**Violation Of New York GBL § 350**

90. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

91. Plaintiff brings this claim individually and on behalf of the proposed Classes against Defendant.

92. New York's General Business Law § 350 prohibits false advertising in the conduct of any business, trade, or commerce.

93. Pursuant to said statute, false advertising is defined as “advertising, including labeling, of a commodity ... if such advertising is misleading in a material respect.”

94. Based on the foregoing, Defendant has engaged in consumer-oriented conduct that is deceptive or misleading in a material way which constitutes false advertising in violation of GBL § 350.

95. Defendant’s false, misleading, and deceptive statements and representations of fact were and are directed to consumers.

96. Defendants’ false, misleading, and deceptive statements and representations of fact were and are likely to mislead a reasonable consumer acting reasonably under the circumstances.

97. Defendants’ false, misleading, and deceptive statements and representations of fact have resulted in consumer injury or harm to the public interest.

98. As a result of Defendants’ false, misleading, and deceptive statements and representations of fact, Plaintiff and the Classes have suffered and continue to suffer economic injury.

99. As a result of Defendants’ violations, Plaintiff and members of the New York Subclass have suffered damages due to said violation because: a) they would not have provided their PII to Defendant had they known Defendant did not use “reasonable physical, technical and administrative measures to protect Personal Information under our control”; (b) their PII has been devalued as a result of being exposed in the data breach; and (c) Plaintiff and members of the Classes must spend considerable time and expenses dealing with the effects of the data breach, and are now at greater risk for future harm stemming from the data breach.

100. On behalf of himself and other members of the New York Subclass, Plaintiff seeks to recover his actual damages or five hundred dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) An Order certifying each of the proposed Classes and appointing Plaintiff and his Counsel to represent the Classes;
- (b) An Order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and the Classes' PII;
- (c) An Order compelling Defendant to employ and maintain appropriate systems and policies to protect consumer PII and to promptly detect, and timely and accurately report, any unauthorized access to that data;
- (d) An award of compensatory, statutory, and punitive damages, in an amount to be determined;
- (e) An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;
- (f) Interest on all amounts awarded, as allowed by law; and
- (g) Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: September 30, 2020

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: /s/ Yitzchak Kopel

Yitzchak Kopel  
Max S. Roberts  
888 Seventh Avenue, Third Floor  
New York, NY 10019  
Telephone: (646) 837-7150  
Facsimile: (212) 989-9163  
Email: ykopel@bursor.com  
mroberts@bursor.com

*Attorneys for Plaintiff*